REMARKS

Claims 16-39 remain in the application, with claims 16 and 28 in independent form. Claims 1-15 have been canceled hereby.

The claims have been carefully reviewed with particular attention to the points raised in the Office Action. It is submitted that no new matter has been added and no new issues have been raised by the present response.

Independent claims 1 and 15 were rejected under 35 U.S.C. § 103(a), as allegedly being unpatentable over U.S. Patent No. 5,535,276 to Ganesan in view of Schneier, "Applied Cryptography," p. 173 (1996) (hereinafter "Schneier"). Accordingly, independent claims 1 and 15 have been canceled with independent claims 16 and 28 being added hereby. It is believed that independent claims 16 and 28 are patentable over the cited art for at least the reasons stated below.

Independent claim 16 relates to a method for mutual authentication of a terminal and a network. A triplet data set is received at the network from an authentication center. The triplet data set includes a first random number (challenge 1), a first response (response 1) and a second response (response 2). The first random number (challenge 1) is sent to the terminal. A first calculated response, sent by the terminal, is received. The first calculated response is calculated by the terminal based on the first random number

(challenge 1). The first calculated response is used as a second challenge (challenge 2). The terminal is authenticated by matching the first calculated response with the first response (response 1). The second response (response 2) is sent to the terminal. The network is authenticated by the terminal by matching a second calculated response, calculated by the terminal based on the first random number (challenge 1) with the second response (response 2).

Ganesan relates to a system for securing communications using cryptography. Asymetric crypto-keys are used to enhance conventional Kerberos authentication systems. The communication is encrypted with the sender and receiver each able to decrypt the message using a corresponding temporary crypto-key.

The cited portion of Schneier relates to random keys, and specifically to keys made of random-bit strings generated by some automatic process.

The cited art, individually or in combination, fails to teach or suggest "**receiving**, at the network, **a triplet data set** from an authentication center, the triplet data set **including** a first random number (**challenge 1**), a first response (**response 1**) and a second response (**response 2**)."

Additionally, the cited art, individually or in combination, fails to teach or suggest that a "**first calculated response** is used as a second challenge (**challenge**

2)."

These features are used in the mutual authentication method as now claimed.

Accordingly, for at least the above-stated reasons, it is respectfully submitted that independent claim 28 and dependent claims 17-27 and 29-39 are patentable over the cited references.

The Office is hereby authorized to charge any fees which may be required in connection with this amendment and to credit any overpayment to Deposit Account No. 03-3125.

Favorable reconsideration is earnestly solicited.

Respectfully Submitted,

Dated: 7/19/05

I hereby certify that this paper is being deposited this date with the U.S. Postal Service as first class mail addressed to:
Commissioner for Patents
P.O. Box 1451
Alexandria, VA 22313-1450

7/19/05
Norman H. Zivin Date
Reg. No. 25,385

Norman H. Zivin
Registration No. 25,385
c/o Cooper & Dunham LLP
1185 Avenue of the Americas
New York, New York 10036
(212) 278-0400
Attorney for Applicants